EXPOSURE DRAFT

PROPOSED DESCRIPTION CRITERIA FOR A DESCRIPTION OF AN ENTITY'S PRODUCTION, MANUFACTURING, OR DISTRIBUTION SYSTEM IN A SOC FOR SUPPLY CHAIN REPORT

Prepared by the AICPA Assurance Services Executive Committee's

SOC for Supply Chain Working Group

CONTENTS

Explanatory Memorandum

Introduction

Due to rapid technological advancement, there is often a high level of interdependence and connectivity between an entity that produces, manufactures, or distributes products (entity) and (*a*) suppliers that provide raw materials, subassemblies, components, other goods, or services, and (*b*) its customers and business partners. These relationships are often considered part of a supply chain.

Although these relationships may increase revenues, expand market opportunities, and reduce costs for the entity, they also result in additional risks to the suppliers, customers, and business partners with whom the entity does business. For example, a cybersecurity attack on the entity's system may also affect its suppliers, customers, and business partners. Likewise, a catastrophic event that shuts down a critical supplier may have a devastating effect on not only the entity but on its customers and business partners. Accordingly, suppliers, customers, and business partners are responsible for identifying, evaluating, and addressing those additional risks. To support their risk assessments, they have begun requesting attestation reports on the entity's system and system controls relevant to security, availability, processing integrity, confidentiality, or privacy.

In response to growing market demand, the AICPA is developing a new examination-level service that CPAs can perform to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the risks of doing business with the entity. Because of the profession's commitment to continuous improvement, public service, and increasing investor confidence, this examination (referred to as a *SOC for Supply Chain examination*) will be voluntary and flexible.

To provide practitioners with performance and reporting guidance for the examination, the Auditing Standards Board (ASB) is working in conjunction with the Assurance Services Executive Committee (ASEC) to develop an attestation guide (referred to as the *SOC for Supply Chain guide* or *guide*). The SOC for Supply Chain examination, which will be described in the guide, will be performed in accordance with the attestation standards. Under those standards, an

attestation engagement is predicated on the concept that a party other than the practitioner[1] makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. The attestation standards state that in an examination engagement, the responsible party (generally, that is *entity management* in a SOC for Supply Chain examination) takes responsibility for the subject matter.

In the SOC for Supply Chain examination, entity management makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. The subject matter of the examination includes the following:

- A description of the entity's system used to produce, manufacture, or distribute products (the description of the system or description) presents the system that was designed and implemented in accordance with the description criteria.

- The controls stated in the description were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria.

Because entity management is ultimately responsible for designing, implementing, and operating the entity's system and the controls within that system, it is also responsible for preparing, and presenting in the SOC for Supply Chain report, the description of the entity's system. Entity management uses description criteria when preparing the description, and the practitioner uses it when evaluating whether the description is in accordance with the description criteria.

This document presents the description criteria for use when preparing the description of the entity's system; it does not present the trust services control criteria against which the effectiveness of system controls is measured and evaluated.[2]

Applying the description criteria in actual situations requires judgment. Therefore, in addition to the description criteria, this document also presents implementation guidance for each criterion.

---

[1] Under those standards, the CPA performing an attest engagement is known as a *practitioner*.

[2] The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* (AICPA, *Trust Services Criteria*) are used to evaluate control effectiveness. The trust services criteria are codified in TSP section 100 of AICPA *Professional Standards.*

The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

The description criteria in this document were promulgated by ASEC. In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*, designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105, *Concepts Common to All Attestation Engagements*,[3] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered to be suitable. Accordingly, ASEC will conclude on whether the description criteria are suitable criteria for preparing and evaluating the presentation of the description of the entity's system in the SOC for Supply Chain examination.

Background

A *SOC for Supply Chain report* is designed to provide intended users with information about the system used to produce, manufacture, or distribute products and the relevant controls within that system. The report is designed to provide users such as the following with information they need to identify, assess, and manage the risks that arise from their relationships with the entity.

- Business customers, including immediate customers or similar business entities further down the supply chain, need information about the entity's system, such as the nature and effectiveness of controls within that system, to (*a*) integrate those controls with the controls within their own systems, and (*b*) determine whether those controls are sufficient to mitigate their own business risks.
- Business partners may include affiliated organizations that are customers or suppliers. Business partners need information about the entity's system and the controls within that system to manage and assess the risks associated with doing business with the entity.

[3] All AT-C sections can be found in AICPA *Professional Standards*.

- Nonregulatory, standard-setting bodies consisting of business customers or business partners that represent their membership (for example, industry consortiums) need information about the entity's system and related controls to better meet the needs of their constituents.

- Others, such as prospective customers and business partners, need information about the entity's system and controls to supplement their supplier selection processes or to ensure the supplier's compliance with regulatory requirements.

Useful Information Included in the Description

A description of the entity's system is designed to provide useful information to enable intended users of the SOC for Supply Chain report to better understand the entity's system. Among other things, the description provides information about the risks that threaten the achievement of the entity's system objectives and the procedures and controls the entity has implemented to manage those risks.

When developing the description criteria, the AICPA recognized the risk that users' need for useful information might result in disclosures that could be used by hostile parties to identify and exploit vulnerabilities in an entity's system. Therefore, the AICPA considered those risks when developing the disclosures called for by the description criteria and attempted to balance those disclosures with the need to protect the entity's information and systems.

Guide for Respondents

ASEC is seeking comments specifically on the nature and extent of information and disclosures contained in the proposed description criteria. Specifically, respondents are asked to respond to the following questions:

1. Are there any unnecessary or otherwise not relevant description criteria or implementation guidance? Please provide a list.

2. Are there any missing description criteria or implementation guidance? Please provide a list.

3. Are there any description criteria or implementation guidance that would result in disclosure of information that would increase the risk of a security event? Please provide a list.

4. Do you have any concerns about the measurability of any of the description criteria or implementation guidance? Please provide a list.

Comments are most helpful when they refer to specific paragraphs or criteria numbers, make specific suggestions for any proposed changes to wording, and include the reasons for the suggestions. When a respondent agrees with proposals in the exposure draft, it would be helpful for the working group to be made aware of this view, as well.

Written comments on the exposure draft should be sent directly to Mimi Blanco-Best, Associate Director – Attestation Methodology and Guidance, at Mimi.Blanco-Best@aicpa-cima.com.

Comment Period

The comment period for this exposure draft ends February 28, 2019.

SOC for Supply Chain Working Group

Chris Halterman, *Chair*
Neal Beggan
Mark Burnette
Jacqueline Easton
Forrest Frazier
Tom Haberman
Jackie Hensgen
Kim Koch
Chris Kradjan
Lev Lesokhin
Heather Paquette
Binita Pradhan
Soma Sinha
Rod Smith
Jeff Trent
Greg Witte
David Wood

AICPA Staff

Erin Mackler

Director

Assurance and Advisory Innovation, SOC Services

Mimi Blanco-Best

Senior Technical Manager

Assurance and Advisory Innovation, SOC Services

Proposed Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report

Introduction

1. The Assurance Services Executive Committee (ASEC), through its SOC for Supply Chain Working Group, has developed a set of benchmarks known as *description criteria*. These description criteria are to be used when preparing and evaluating a description of an entity's production, manufacturing, or distribution system (description) in a SOC for Supply Chain examination.[1]

2. A SOC for Supply Chain report is intended to provide report users with information about a system used to produce, manufacture, or distribute goods and the relevant controls within that system.[2] Such information maybe be used to identify, assess, and manage the risks that arise from doing business with the entity. The information may relate to one or more of the following categories: security, availability, or processing integrity of that system.[3] In some situations, the information may also address the privacy or confidentiality of information used in the operation of that system.[4]

---

[1] In a SOC for Supply Chain examination, the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), codified as TSP section 100, are used to evaluate the effectiveness of controls. The term *applicable trust services criteria* refers to the criteria associated with one or more of the categories included within the scope of the examination. Although this document does not discuss the use of the trust services criteria in the SOC for Supply Chain examination, the guide does.

[2] Throughout this document, the terms *product* and *good* are used interchangeably and refer to both physical or intangible products or goods (for example, software).

[3] In a SOC for Supply Chain examination, the processing integrity category addresses the system used to produce, manufacture, or distribute goods, including the components of that system (for example, hardware, tooling, software, and information).

[4] As discussed in footnote 1, these are the five categories addressed by the *2017 Trust Services Criteria*.

3. In a SOC for Supply Chain examination, entity management prepares a description of the system as it relates to one or more of those categories and makes an assertion about the description of the system and the effectiveness of controls within that system. The practitioner performs procedures to obtain sufficient appropriate evidence about whether the description is in accordance with the description criteria presented in this document and whether the controls are effective; such evidence forms the basis for the practitioner's opinion on the description.

4. The description criteria were developed to be used in conjunction with the SOC for Supply Chain examination described in the AICPA Guide *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System* (guide).

5. Because applying the description criteria requires judgment, this document also presents implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. This guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the entity and its environment when applying the description criteria.

Applicability and Use of the Description Criteria

SOC for Supply Chain Examination

6. A SOC for Supply Chain examination addresses a system used by an entity to produce, manufacture, or distribute goods (system). Examples of entities that produce, manufacture, or distribute goods include the following:

    - *Producer.* Producers include entities that extract raw materials from the earth through operations that remove metals, mineral, and aggregates from the earth (such as oil and gas extraction, mining, dredging, and quarrying); produce food, feed, fiber, and other products by the cultivation of certain plants and the raising of domesticated animals (livestock); and develop software for onsite installation.

    - *Manufacturer.* Manufacturers include entities that transform raw materials or components into other components or finished goods for use or sale using labor and machines, tools, chemical and biological processes, fabrication, or formulation.

The components or finished goods may be sold to other manufacturers for the production of other products such as aircraft, computers or computer parts, household appliances, furniture, sports equipment, or automobiles. In other cases, the finished goods may be sold to wholesalers that, in turn, sell them to retailers, that then sell them to end users and consumers.

- *Software developer*. Software developers include entities that develop and sell software designed to be implemented by users with minimal to no customization of the underlying computer code.

- *Distributor*. Distributors include entities that provide or manage all or a significant part of another entity's logistics, including one or a combination of the following: inbound freight; customs; warehousing; inventory management; order fulfillment, including picking and repackaging items; distribution; or outbound freight. Such companies may be referred to as *third-party logistics (3PL or TPL) companies*.

7. The SOC for Supply Chain examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*.[5] In that examination, the practitioner expresses an opinion about whether the

   a. description is presented in accordance with the description criteria, and

   b. controls were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria.[6,7]

8. A SOC for Supply Chain examination is predicated on the concept that because entity management is ultimately responsible for developing, implementing, and operating the entity's system, entity management is responsible for developing and presenting a

[5] All AT-C sections can be found in AICPA *Professional Standards*.

[6] See footnote 1.

[7] The term *effectiveness of controls* encompasses controls that are both suitably designed and operating effectively to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria. Suitably designed controls, if complied with satisfactorily, provide reasonable assurance of achieving the entity's system objectives; suitably designed controls operate effectively if they provide reasonable assurance of achieving the entity's system objectives.

description of the entity's system. Entity management uses the description criteria in this document when preparing the description of the entity's system; the practitioner uses the description criteria when evaluating whether the description is presented in accordance with the description criteria.

Contents of a SOC for Supply Chain Report

9. The description of the entity's system prepared in accordance with the description criteria in this document is included in the SOC for Supply Chain report, which also includes the following:

    a. Entity management's assertion about the description and whether controls stated in the description were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria

    b. The practitioner's opinion on the description and whether controls stated in the description were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria

    c. A description of the testing procedures performed by the practitioner and the results thereof

10. The inclusion of a description of testing procedures performed by the practitioner and the results thereof in the SOC for Supply Chain report creates a risk that users, other than the intended users described in paragraphs .12 and .15, may misunderstand the content of the report, including the practitioner's opinion. For that reason, entity management and the practitioner should agree on the intended users of the report and on the fact that the practitioner's report will be restricted to their use.[8]

Intended Users of a SOC for Supply Chain Report

11. The purpose of a SOC for Supply Chain examination is to provide useful information to enable users of goods produced, manufactured, or distributed by an entity to better

[8] Paragraph .64 of AT-C section 205, *Examination Engagements*, refers to these intended users as *specified parties*.

understand and manage the risks, including cybersecurity risks, arising from their business relationships with the entity.

12. Intended users of a SOC for Supply Chain report are as follows:

    a. Business customers, including immediate customers or similar business entities further down the supply chain, that do the following:

        i. Use the system's products as components of their production and manufacturing systems (for example, production machinery)

        ii. Use the system's products as inputs to their products (for example, computers used in automobiles)

        iii. Use the system's products as a part of their service delivery (for example, IV bags used by a hospital)

        iv. Resell the products

        v. Rely on a physical distribution system for products used as inputs to products

    Business customers need information about the entity's system, including the nature and effectiveness of controls within that system, to integrate those controls with the controls within their own systems and to determine whether those controls are sufficient to mitigate their own business risks.

    b. Business partners of an entity that

        i. are dependent on a customer or distributor for their sales

        ii. license the use of their intellectual property to others

    Business partners may include affiliated organizations that are customers or suppliers. Business partners need information about the entity's system and the controls within that system to manage and assess the risks associated with doing business with the entity.

c. Nonregulatory, standard-setting bodies consisting of business customers or business partners that represent their membership (for example, industry consortiums)

Those users need information about the entity's system and related controls to better meet the needs of their constituents.

13. The limited population of users identified in the previous paragraph need certain knowledge and understanding of the entity and the system used to produce, manufacture, or distribute goods, among other matters, to understand the SOC for Supply Chain report. Without such knowledge, users are likely to misunderstand the report, the assertions made by entity management, details about the tests performed by the practitioner and the results of those tests, and the practitioner's opinion, all of which are included in the SOC for Supply Chain report. For that reason, as discussed in paragraph .10, the practitioner's report would be restricted to the use of the intended users.

14. The expected knowledge of the intended users of a SOC for Supply Chain report ordinarily includes the following:

a. The nature of the goods produced, manufactured, or distributed by the entity

b. Internal control and its limitations

c. The applicable trust services criteria

d. The risks that may threaten the achievement of the entity's system objectives and how controls address those risks

The practitioner's report is restricted to the use of the specified users in accordance with AT-C section 205.

15. Parties other than those identified in paragraph .12 may also have the requisite knowledge and understanding identified in the preceding paragraph. For example, prospective customers and business partners, who intend to use the information contained in the SOC for Supply Chain report to determine whether to do business with the entity or to comply with regulatory requirements for supplier acceptance, may have gained such knowledge while performing due diligence.

16. Other parties, however, may want to use the SOC for Supply Chain report but lack the requisite knowledge and understanding described in paragraph .14. Investors, potential

investors, consumers, and members of the public (general users), for example, may not have the same level of knowledge as the intended users identified in paragraphs .12 and .15; therefore, such users are more likely to misunderstand the SOC for Supply Chain report. In addition, inclusion in the report of a description of the practitioner's tests and the results of those tests increases the risk of misunderstanding. Consequently, such other parties are not considered primary intended users of the SOC for Supply Chain report.

Suitability and Availability of the Description Criteria

17. The description criteria in this document were promulgated by ASEC. In establishing and developing these criteria, ASEC has followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*, designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered to be suitable. Accordingly, ASEC will conclude on whether the criteria in this document are suitable for preparing and evaluating the presentation of the description of a system in a SOC for Supply Chain examination. Because ASEC intends to publish the description criteria and make them available to the public, they will be considered available to report users. Therefore, the description criteria have been designed to meet the definition in paragraph .25*b*(ii) of AT-C section 105 for criteria that is both suitable and available for use in an attestation engagement.

18. According to the attestation standards, the attributes of suitable criteria are as follows:[9]

    - *Relevance.* Criteria are relevant to the subject matter.
    - *Objectivity.* Criteria are free from bias.
    - *Measurability.* Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.

[9] Paragraph .A42 of AT-C section 105, *Concepts Common to All Attestation Engagements*.

- *Completeness.* Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect users' decisions made on the basis of that subject matter.

19. In addition to being suitable, paragraph .25*b* of AT-C section 105 indicates that the criteria used in an attestation engagement should be available to intended users. The publication of the description criteria makes the criteria available to intended users. Accordingly, ASEC has concluded that the description criteria presented in this document are suitable and available for use in a SOC for Supply Chain examination.

Preparing and Evaluating the Description of the Entity's Production, Manufacturing, or Distribution System in Accordance With the Description Criteria

20. As previously discussed, a description of the entity's system presented in accordance with the description criteria is designed to enable intended users of the SOC for Supply Chain report to better understand the entity's system. Among other things, the description provides information about the risks that threaten the achievement of the entity's system objectives and the procedures and controls the entity has implemented to manage those risks. The description is prepared by entity management from documentation supporting the system of internal control and system operations, as well as consideration of the policies, processes, and procedures within the system.

21. There is no prescribed format for the description. Management may organize the description in a variety of ways, provided that disclosures called for by the description criteria are met. Flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof also may be used to supplement the narratives contained within the description.

22. The extent of disclosures included in the description may vary depending on the size and complexity of the entity and its activities. In addition, the description need not address every aspect of the entity's system for producing, manufacturing, or distributing goods, particularly if certain aspects of the system are not relevant to intended users or are beyond the scope of the SOC for Supply Chain examination. For example, disclosures about an entity's processes related to billing to customers for the manufactured products are unlikely to be relevant to intended users. Similarly, although the description includes procedures

within both manual and automated systems by which goods are produced, manufactured, or distributed, it need not necessarily disclose every step in those processes.

23. Ordinarily, a description of an entity's system in a SOC for Supply Chain examination is in accordance with the description criteria when it (*a*) describes the system that the entity has implemented (that is, placed in operation) for producing, manufacturing, or distributing goods, (*b*) includes information about each description criterion to the extent it is relevant to the system being described, and (*c*) does not inadvertently or intentionally omit or distort information in a manner that may be misleading to intended users. Although the description should include disclosures about each description criterion, such disclosures are not intended to be made at such a detailed level that they might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the entity's ability to achieve its system objectives. Instead, the disclosures are intended to enable intended users to understand the nature of the risks faced by the entity and the potential impact of the realization of those risks.

24. A description is not in accordance with the description criteria if, for example, it (*a*) states or implies that certain IT components exist when they do not, (*b*) states or implies that certain processes and controls have been implemented when they are not being performed, or (*c*) contains statements that cannot be objectively evaluated (for example, advertising puffery).

25. In certain circumstances, additional disclosures may be necessary to supplement the description. Entity management's decisions about whether such additional disclosures are necessary, and the practitioner's evaluation of entity management's decisions, involve consideration of whether the disclosures may affect information that is likely to be relevant to the decisions of intended users. Examples of additional disclosures that may be necessary include the following:

    - Significant interpretations made in applying the description criteria in the specific circumstances of the SOC for Supply Chain examination (for example, what constitutes a security event or incident)
    - Subsequent events, depending on their nature and significance

Materiality Considerations When Preparing and Evaluating Whether the Description Is in Accordance With the Description Criteria

26. As discussed in paragraph .05, applying the description criteria requires judgment. The practitioner's judgment is informed by the identification of the intended users of the report and the types of decisions they are likely to make based on the SOC for Supply Chain report. As previously discussed in paragraphs .12 and .15, there may be a variety of intended users of a SOC for Supply Chain report. A description in accordance with the description criteria presented in this document is intended to meet the common informational needs of those intended users. For that reason, an understanding of the perspectives and informational needs of the broad range of intended users is necessary to determine whether the disclosures are likely to result in a presentation that will meet the common information needs of those users.

27. When evaluating whether the description is presented in accordance with the description criteria, entity management considers whether misstatements in the description, individually or in the aggregate, could reasonably be expected to influence relevant decisions of intended users. In this context, misstatements ordinarily include the omission of relevant information, errors in presentation, or the presentation of information in a manner that is misleading to users. For example, in a SOC for Supply Chain examination on controls relevant to privacy, entity management may discover that it has failed to describe a principal commitment involving compliance with the European Union's General Data Protection Regulation. Because such information could reasonably be expected to influence the decisions of intended users, entity management may conclude that the omission of such information causes the description to be materially misstated. In that case, entity management would amend the description by including the relevant information.[10]

28. Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions are presented in narrative form. Therefore, materiality considerations are mainly qualitative in nature. Examples of qualitative factors that may be considered include whether

[10] If the description has been prepared to meet the informational needs of a specific subset of the intended users described in paragraphs .12 and .15 (and the report is restricted to those specific users), entity management considers whether misstatements (including omissions) may affect the decisions of the specific subset of report users.

- the description of the entity's system includes the significant aspects of system processing.
- the description is prepared at a level of detail likely to be meaningful to intended users (that is, the precision of the disclosures).
- each of the relevant description criteria in paragraph .30 has been addressed without using language that omits or distorts the information.
- the characteristics of the presentation are appropriate because the description criteria allow for variations in presentation.

Description Criteria and Related Implementation Guidance

29. To be presented in accordance with the description criteria, a description ordinarily needs to disclose information about each of the requirements (criteria) presented in the left column of the following table, to the extent that the criterion is applicable to the system and the trust services categories included within the scope of the examination. (Materiality considerations are discussed in the previous section beginning at paragraph .26.)

30. The implementation guidance in the right column of the following table presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, entity management is advised to carefully consider the specific facts and circumstances of the entity and the nature of the goods produced, manufactured, or distributed when applying the description criteria in a SOC for Supply Chain examination.

Description Criteria	***Implementation Guidance***
The description contains the following information applicable to the system and the trust services category or categories addressed by the description.	When making judgments about the nature and extent of disclosures to include, consider the following:

DC 1: The types of goods produced, manufactured, or distributed by an entity and, if relevant, the characteristics of the production, manufacturing, or distribution processes	An entity describing its system may produce, manufacture, or distribute a variety of products. Consequently, the description needs to include information about the types of products produced, manufactured, or distributed by the entity and the system or systems used to produce, manufacture, or distribute the products. Furthermore, the disclosures are only made to the extent that they relate to the trust services category or categories addressed by the description. The description can address a single model, product, or commercial off-the-shelf (COTS) application, the system for a production line, or products produced by a single manufacturing facility or physical plant. The types of products will depend on the nature of the entity: • *Producer*: Producers include entities that extract raw materials from the earth through operations that remove metals, mineral, and aggregates from the earth (such as oil and gas extraction, mining, dredging, and quarrying); produce food, feed, fiber, and other products by the cultivation of certain plants and the raising of domesticated animals (livestock); and develop software for onsite installation. • *Manufacturer*: Manufacturers include entities that transform raw materials or components into other components or finished goods for use or sale using labor and machines, tools, chemical and biological processes, fabrication, or formulation. The components or finished goods may be sold to other manufacturers for the production of other products such as aircraft, computers or computer parts, household appliances, furniture, sports equipment, or automobiles. In other cases, the finished goods may be sold to wholesalers, that in turn, sell them to retailers, that then sell them to end users and consumers. • *Software developer*: Software developers include entities that develop and sell software designed to be implemented by

	users with minimal to no customization of the underlying computer code. • *Distributor*: Distributors include entities that provide or manage all or a significant part of another entity's logistics, including one or a combination of the following: inbound freight; customs; warehousing; inventory management; order fulfillment, including picking and repackaging of items; distribution; or outbound freight. Such companies may be referred to as *third-party logistics (3PL or TPL) companies*.
DC 2: The principal product specifications, commitments, and requirements, and production, manufacturing, or distribution commitments and requirements (system objectives)	A system of internal control is evaluated using the trust services criteria within the context of the entity's ability to achieve its business objectives and sub-objectives. In the context of a description of an entity's production, manufacturing, or distribution system, an entity's objectives are referred to as *system objectives.* An entity's system objectives generally focus on meeting customer needs and expectations. Depending upon the trust services category or categories addressed by the description, the objectives and sub-objectives often relate primarily to the following: *a.* Commitments regarding the protection of the system from cybersecurity risks *b.* The product meeting the product specifications that have been communicated to or agreed-upon with customers *c.* The product's conformity with any other commitments made to customers *d.* The product's conformity with product requirements established by the entity, law or regulation, industry standards, or customers' requirements *e.* The product's availability in the quantities and at the times agreed upon with customers *f.* The achievement of delivery commitments made to customers, including the timing of delivery, storage and transportation commitments, and the system requirements necessary to achieve those commitments

	g. Distribution of the product in accordance with applicable laws and regulations regarding timing, storage, and transportation *h.* The achievement of other objectives established by the entity for the manufacturing, production, or distribution system Although entity management is responsible for designing, implementing, and operating controls to provide reasonable assurance that it achieves its system objectives, entity management may limit disclosures to its principal system objectives. The purpose of disclosure of the principal system objectives is to help users understand the objectives that drive the operation of the system and how the applicable trust services criteria were used to evaluate whether controls were effective. *Product specifications*. For a product, system objectives include producing or manufacturing a product that meets product specifications to the extent that those specifications relate to the trust services category or categories addressed by the description. Product specifications may address the physical characteristics or functionality of a product and are often published, specified in contracts, or otherwise communicated to customers. *Production, manufacturing, or distribution specifications*. For customers and business partners, it may be important to understand not only whether the product meets its specifications but how production, manufacturing, or distribution occurs. For example, a business partner may establish specifications for the entity's use of the business partner's intellectual property during the production process. Or, a pharmaceutical entity may establish specifications for a product to be maintained at a specific temperature during the distribution process. To the extent that those specifications relate to the trust services category or categories addressed by the description, meeting production, manufacturing, or distribution specifications are likely to be objectives of the system. *Other commitments*. In addition to meeting specific product, production, manufacturing, or distribution specifications, entities often make other commitments to customers and business partners. To the extent that those commitments relate to the trust

	services category or categories addressed by the description, the system objectives include those commitments. For example, an entity may make commitments about conforming with a variety of other standards and criteria, such as the risk management framework issued by the National Institute of Standards and Technology (NIST), the cybersecurity standards issued by the International Standardization Organization (ISO), or the FDA regulations on electronic records and electronic signatures included in Title 21 CFR Part 11. It may also make commitments on many different aspects of the product or its distribution, including commitments related to a product's performance specifications and availability. An entity may also make commitments related to one or more of the trust services categories addressed by the description. As an example, if controls over privacy are addressed by the description, an entity may make commitments such as the following: • The entity will not process or transfer information without obtaining the data subject's consent. • The entity will provide a privacy notice to customers once every six months or when there is a change in its business policies. The commitments an entity makes to customers, business partners, and others are based on the needs of those entities. In identifying the commitments to be disclosed, entity management may begin by reviewing the specific commitments it has made to customers and business partners. Commitments may be communicated in many ways, such as through contracts, service level agreements, and published policies (for example, a privacy policy). No specific form of communication is required. As previously discussed, entity management may limit its disclosures to those commitments that are relevant to the broad range of users (that is, the principal commitments). For example, an entity often makes the same product availability commitment to its customers. Because information about the availability commitment is likely to be relevant to customers, entity

	management would describe that principal availability commitment in the description when the description addresses availability. In other cases, however, an entity may make a different commitment (for example, about product availability) to a specific customer. Entity management ordinarily would not disclose that commitment in the description because it is unlikely to be relevant to most of its customers. Because that commitment is not disclosed in the description, the specific customer understands that the evaluation of the effectiveness of controls was made based on the entity's achievement of its principal availability commitments (that is, those common to most of the entity's customers); therefore, the specific customer may need to obtain additional information from the entity regarding the achievement of its specific availability commitment. When the description addresses privacy, entity management discloses the commitments and system requirements identified in the entity's privacy notice or privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to users if entity management describes the purposes, uses, and disclosures of personal information as permitted by agreements. *Product requirements.* In addition to specifications and commitments regarding products, the product itself may need to meet other requirements to meet those specifications or commitments. The product may also be subject to legal or regulatory requirements. For example, COTS software may need to meet a specific set of requirements to function properly with a particular operating system. *Production, manufacturing, or distribution requirements.* In addition to specifications and commitments, production, manufacturing, or distribution systems may be subject to requirements about how the system should function to accomplish the following: • Meet product specifications, commitments, or requirements.

	• Meet the entity's production, manufacturing, or distribution commitments to customers and others (such as customers' customers) • Meet the entity's commitments to supplier and business partners • Comply with applicable laws and regulations, and guidelines of industry groups, such as business or trade associations • Achieve other objectives of the entity that are relevant to the trust services category or categories addressed by the description Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations. Examples of system requirements include the following: • Workforce member background checks established in government regulations for handling hazardous materials • Temperature ranges acceptable for the operation of process during production • Software quality and security standards such as those issued by the Open Web Application Security Project (OWASP), the Consortium for IT Software Quality™ (CISQ™), and the ISO. • Labeling and tagging standards, including any associated metadata requirements, established by industry groups or other bodies • Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA)

	System requirements may result from the entity's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between production and quality control approval creates system requirements regarding user access administration). The principal system requirements that need to be disclosed are those that are relevant to the trust services category or categories addressed by the description and likely to be relevant to users. In identifying which system requirements to disclose, entity management may consider internal policies that are relevant to the system being described, key decisions made in the design and operation of the system, and other business requirements for the system. For example, internal requirements related to the profit margin for the products associated with the system ordinarily would not be relevant to users and, therefore, need not be disclosed.
DC 3: For identified system incidents that (*a*) were the result of controls that were not effective or (*b*) otherwise resulted in a significant failure in the achievement of one or more of the entity's system objectives during the period of time addressed by the description,[11] the following information: *a.* Nature of each	Judgment is needed when determining whether to disclose an incident. However, consideration of the following matters as they relate to the system and the trust services category or categories being described may help make that determination: • Whether the incident resulted from one or more controls that did not provide reasonable assurance that the entity achieved one or more of its system objectives • Whether the incident resulted in a significant failure in the achievement of one or more of the entity's system objectives • Whether public disclosure of the incident was required (or is likely to be required) by laws or regulations • Whether the incident had a material effect on the entity's

[11] If the description addresses only implemented controls as of a point in time, this disclosure relates to identified system incidents that (*a*) were the result of controls that were not effective or (*b*) otherwise resulted in a significant failure in the achievement of one or more of the entity's system objectives as of the date of the description.

incident *b.* Timing surrounding the incident *c.* Extent (or effect) of the incident and its disposition	financial position or results of operations and required disclosure in a financial statement filing • Whether the incident resulted in sanctions by any legal or regulatory agency • Whether the incident resulted in the entity's withdrawal from material markets or cancellation of material contracts Disclosures about identified system incidents are not intended to be made at a detailed level, which might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the entity's ability to achieve its system objectives. Rather, the disclosures are intended to enable users to understand the nature of the risks faced by the entity and the impact of the realization of those risks. Assume that the entity identified a security breach that resulted in its failure to achieve one or more of its system objectives. The breach, which occurred six months prior to the start of the period addressed by the description, had not been fully remediated during the period addressed by the description. In this example, entity management would likely need to disclose the incident in the description to enable users to understand the nature of the risks faced by the entity and the impact of the realization of those risks. In addition, entity management should consider whether to disclose known incidents at a supplier, regardless of whether entity management has elected to use the inclusive or carve-out method.
DC 4: Significant risks that affect the entity's production, manufacturing, or distribution	Disclosures about significant risks are only made to the extent that they relate to the trust services category or categories addressed by the description. Significant risks include those arising from (1) characteristics of the production, manufacturing, or distribution system and underlying information systems, use of suppliers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) physical, environmental, technological, organizational, and other changes during the period addressed by

	the description. *Characteristics of the production, manufacturing, or distribution system, underlying information systems, use of suppliers, and delivery channels.* Disclosures about the risks related to these matters may include the following: • Nature and importance of key product and production specifications, commitments, and requirements • Use of supporting information systems such as overall architecture, code-to-control production machinery, cloud computing, and other IT-hosted services • Types of production, manufacturing, or distribution equipment, related technology and infrastructure used, and the source of such equipment, applications, and infrastructure (for example, whether software is internally developed or purchased without modification) • Use of suppliers (for example, raw materials or component suppliers such as subassemblies or embedded technology and logic) that produce, manufacture, or distribute products or software, including confidential intellectual property • Types of physical and logical access of third parties to plants, locations, and information systems • Nature of external-facing web applications and the nature of applications developed in-house • Dependency on strategically significant production, manufacturing, or distribution equipment and systems that are no longer made or supported or would be difficult to repair or replace in the event of failure • Dependency on IT equipment and information systems critical to the production, manufacturing, or distribution processes and those based on emerging technologies

	Organizational and customer characteristics. Disclosures about the risks related to organizational and customer characteristics may include the following: • The size and structure of the entity (for example, centralized versus decentralized, insourced, or outsourced) and changes to that structure resulting in a change to internal control over the system (for example, a change to the legal entity) • Types of customer groups, business partners, and other third parties, such as suppliers, that are significant to the operation of the system products or services • Whether the entity's production, manufacturing, or distribution assets, employees, customers, suppliers, or business partners are in countries or regions deemed high risk by entity management as part of its risk assessment process • The distribution of responsibilities related to the production, manufacturing, or distribution risk management program between business functions (for example, operating units, risk management, production management, and legal) • Business units with production, manufacturing, or distribution systems administered under a separate entity management structure (for example, outside of a centralized production, manufacturing, or distribution function) *Physical, environmental, technological, organizational, and other changes*. Disclosures about the risks related to physical, environmental, technological, organizational, and other changes at the entity and in its environment during the period addressed by the description may include the following: • Changes to the entity's principal production, manufacturing, or distribution methods • Changes to business unit, production, manufacturing, or distribution, supporting IT, and related personnel

	• Changes to the risk assessment and controls monitoring processes resulting from the failure of controls designed to achieve product specifications, commitments, and requirements • Significant changes to the entity's production, manufacturing, or distribution processes, supporting IT architecture and applications, and the processes and systems used by suppliers • Changes to legal and regulatory requirements that affect the production, manufacturing, or distribution systems • Divestures and other cessation of operations, particularly those that have ongoing service support obligations for production, manufacturing, or distribution related to those operations (if any), and the status of those activities
DC 5: Inputs to the system (raw materials and other inputs) and the components of the system used to produce, manufacture, or distribute the product. Components include the following: *a.* Infrastructure *b.* Software *c.* People *d.* Procedures *e.* Data	Disclosures about system components are only made to the extent that they relate to the trust services category or categories addressed by the description. As discussed previously, the description may address the system for a product line or products produced by a single manufacturing facility or physical plant. Depending on the nature of the processes, the description may need to address the system or systems used to produce or manufacture products from the beginning of the production cycle (raw materials or inputs) to the distribution of the finished goods to customers, as discussed separately in the following text. Entities that produce or manufacture products may use systems to distribute the products they produce or manufacture to customers (for example, an entity that distributes feature films or game DVDs). In contrast, entities may contract with a 3PL company to distribute their products (for example, an air bag manufacturer that contracts with XXX Trucking to transport the finished product to the final customer, or car manufacturer).

	Other entities may use systems to distribute products that have been produced or manufactured by other entities. In some cases, they may repackage products produced or manufactured by others before transporting them to the final customers. In other cases, they may only provide transportation services for products manufactured or produced by others (for example, an express shipping company) in instances in which only transportation services are provided. If transformative services are not provided by the distributor, then those processes may not be considered processes related to production, manufacturing, or distribution and may be better addressed by a SOC 2® examination.[12] Often, for products to meet specifications, commitments, and requirements, electronics and the onboard logic within the product need to meet certain requirements. In describing the system, entity management may need to consider those portions of the system used to create and implement executable logic contained in those electronics, whether in software or hardware, that is embedded in the product, as well as the hardware and software used to produce and distribute the product. A description may address one or more systems used to distribute products. A description may also address each system used to distribute products produced or manufactured within a specific manufacturing facility or physical plant. For entities that distribute products, the characteristics of the distribution system to be included in the description may include the following matters, as applicable: • The geographic region served • Transportation methods used • Types of products transported

[12] The performance and reporting requirements for an examination of controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy are found in AT-C section 205. The AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* contains application guidance for practitioners.

	• Whether the entity repackages products produced or manufactured by others • Whether the entity provides special handling services System components may also be described using specific technical terms that will help create a clearer understanding of the entity's system and system boundaries. The following paragraphs provide additional guidance on disclosures related to the components of the system or systems that may be included in the description. *Infrastructure.* Disclosures about the infrastructure component of a system (that is, production and distribution equipment, including IT equipment used to support production, manufacturing, or distribution) include matters such as the collection of physical or virtual resources that supports an overall production, manufacturing, or distribution environment, including the physical environment and related structures, production and manufacturing systems, IT, and related hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the entity uses to produce, manufacture, or distribute the products. *Software.* Disclosures about software used in the production, manufacturing, or distribution process include matters such as the application programs (including, if applicable, industrial control systems), programmable logic on devices used in production, the IT system software that supports those application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop and laptop applications. *People.* Disclosures about the people component include the personnel involved in the governance, entity management, operation, security, and use of the system (business unit personnel, production line personnel, developers, operators, customer personnel, supplier personnel, and managers). *Procedures.* Disclosures about the automated and manual procedures implemented by the entity and primarily relating to

	those through which production, manufacturing, or distribution occur. These include, as appropriate, procedures through which production and manufacturing is initiated, authorized, and occurs; the procedures through which products are distributed; and the processes by which reports and other information are prepared and distributed. A *process* consists of a series of linked procedures designed to accomplish a goal (for example, the process for assembling a product or managing third-party risks). *Procedures* are the specific actions undertaken to implement a process (for example, the procedure to assess and manage the requisition and engagement of suppliers). For that reason, entity management may find it easier to describe procedures in the context of the process of which they are a part. *Policies* are entity management or board statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. The entity deploys control activities through policies that establish what is expected and procedures that put policies into action. *Data.* Disclosures about the data component include the types of data used by information systems, transaction streams, files, databases, tables, and output used or processed by such systems. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following: • The principal types of data created, collected, processed, transmitted, used, or stored by the entity and the methods used to collect, retain, disclose, dispose of, or anonymize the data • Personal information that warrants security, data protection, or breach disclosures based on laws or commitments (for example, personally identifiable information, protected health information, and payment card data)

	• Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants security, data protection, or breach disclosures based on laws or commitments When the description addresses controls over confidentiality and privacy, entity management would address, at a minimum, all the system components as they relate to the information life cycle of the confidential and personal information used in producing, manufacturing, or distributing the products within well-defined processes and informal ad hoc procedures. *Raw materials and other inputs.* Although raw materials are not part of the system, they are often necessary for a product to be produced or manufactured. For that reason, it is sometimes useful to describe the use of raw materials or other inputs (for example, purchased components) in the production or manufacturing process. Such disclosures often assist users in obtaining a better understanding of the production or manufacturing system addressed by the description. *Boundaries of the system.* Not all activities performed at the entity are part of the system being described. Determining the functions or processes that are outside the boundaries of the system and describing them in the description may be necessary to prevent users from misunderstanding the boundaries of the system. Therefore, if there is a risk that users might be confused about whether a specific function or process is part of the system being described, the description needs to clarify which processes or functions are included in the examination. For example, the following functions or processes at the entity may be outside the boundaries of the system being described: • Processes used to transport work in process between production steps • The process used to invoice customers for the products provided by the entity

	• Processes used to collect and report on sustainability matters that do not directly affect the finished product *Third-party access.* Suppliers, business partners, customers, and other third parties often store, process, and transmit sensitive data or otherwise access an entity's system. These third parties may provide components of the system. Entity management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the entity's system.
DC 6: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the entity's system objectives were achieved	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), presents the criteria for each of the trust services categories. A description is presented in accordance with this criterion when it includes information about each of the criteria related to the trust services category or categories addressed by the description (applicable trust services criteria), including controls related to the control environment, risk assessment process, information and communication, monitoring activities, and control activities. For example, if the description addresses availability, entity management would provide information about the controls it has implemented to address the common criteria in the trust services criteria and the additional trust services criteria for availability.
DC 7: If a customer's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives would be achieved, those complementary customer controls	Customers often have a role in a production, manufacturing, or distribution process. Fulfilling those responsibilities is necessary for the customer to meet its goals in using an entity as a supplier or distributor. For example, the customer of a logistics company that provides fulfillment services is responsible for providing complete and accurate recipient information and communicating the items to be packaged and delivered. Such responsibilities are referred to as *customer responsibilities*. Because customer responsibilities can be voluminous, they are not ordinarily disclosed in the description; rather, they are usually

	communicated through product documentation or user manuals. However, entity management would ordinarily disclose in the description the types of communications it makes to customers about their responsibilities. In most cases, the successful performance of customer responsibilities is not necessary for the entity to achieve its system objectives. In limited circumstances, however, a customer must have controls in place to provide reasonable assurance that its customer responsibilities are performed in a defined manner for the entity to achieve its system objectives. Such controls are referred to as *complementary customer controls* (CCCs). Consider, for example, a situation in which an entity installs a server at a customer's data center to support the customer's access to the entity's production management system. The customer needs to implement physical access controls at its customer site to protect the components of the entity's system installed at its data center for the entity to achieve its system objectives based on trust services criterion CC6.4, which states the following: > The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to achieve the entity's objectives. When CCCs are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved, those CCCs are disclosed in the description along with the applicable trust services criteria to which they relate. Disclosures about CCCs are made only to the extent that they relate to the trust services category or categories addressed by the description. In some situations, a customer responsibility that appears to be a CCC is not. For example, a manufacturer may permit a customer's employees to access information systems and alter its production schedules. If a customer access administrator is responsible for issuing employee credentials, and all actions performed by customer

	employees are the responsibility of the customer, the achievement of the entity's system objectives does not depend on the authorized and appropriate use of the customer employee credentials based on trust services criterion CC6.2, which states the following: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
DC 8: If a supplier's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved and *a.* the entity is using the carve-out method (most common), the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. Each of the applicable trust services	An entity that produces, manufactures, or distributes products obtains raw materials, components, or other goods (for example, production equipment) from suppliers. It may also outsource various processing functions (such as the provision of IT networks) to service providers. A supplier may be a separate entity that is external to the entity or may be a related entity, for example, a subsidiary of the same company that owns the entity. In most cases, an entity is likely to have effective controls over the quality of raw materials, subassemblies, other goods, and system components (including services) obtained from suppliers to provide reasonable assurance of achieving its system objectives. Examples of situations in which an entity may have effective controls over a supplier's goods or services to achieve the system objectives include the following: • An entity has robust controls, including change management controls, over a system used by a supplier to produce new software, which the entity then uses in its production process. In that case, the entity's monitoring of the supplier's system and controls is sufficient for the entity to achieve its system objectives. • A supplier is responsible for performing quarterly maintenance on an entity's back-up power system in an examination that addresses availability. If the entity implements its own monitoring controls over the supplier's

criteria that are intended to be met by controls at the supplier iii. The types of controls that entity management assumed, in the design of the entity's system, would be implemented by the supplier and are necessary, in-combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved (commonly referred to as *complementary supplier controls* or CSCs) *b.* the entity is using the inclusive method, the following: i. The nature of	controls, then the supplier's controls would not be necessary for the entity to achieve its system objectives. • An entity outsources its application development testing to a supplier and stipulates in its supplier contract that the supplier is responsible for performing certain controls that the entity believes are necessary to address the risks related to doing business with the supplier. The entity designates an entity employee to oversee the outsourced services, and that employee compares the supplier's test plans, test scripts, and test data to the entity's application change requests and detailed design documents. The designated entity employee also reviews the results of testing performed by the supplier before changes to the application are approved by the supplier and submitted to the entity for user acceptance testing. The supplier's controls may not be necessary for the entity to assert that its controls provide reasonable assurance that the entity's availability commitments were achieved based on the applicable trust services criteria. In other situations, however, the entity may not have such controls. For example, an entity may be sourcing subassemblies that contain embedded software and may be unable to directly assess the quality and security of that software. In that case, the entity would delegate certain responsibilities to the supplier and expect the supplier to perform specific controls over the processes used to produce or deliver the subassemblies. As a result, effective supplier controls may be necessary for the entity to achieve its system objectives. *Carve-out method*. When the controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the system objectives, such controls are referred to as *complementary supplier controls* (CSCs). Because CSCs are important to report users, they are disclosed in the description. The most common method for presenting CSCs is to include only those processes and controls whose performance is the responsibility of the entity and identify the CSCs that the entity expects suppliers to implement. This method is known as the *carve-out method*.

the products produced, manufactured, or distributed or the services provided by the supplier ii. The portions of the system that are attributable to the supplier iii. Relevant aspects of the supplier's infrastructure, software, people, procedures, and data iv. The controls at the supplier that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives are achieved	When using the carve-out method, the description identifies the types of CSCs that the supplier is expected to implement and the trust service criteria affected by them. Consideration also may be given to disclosing the identity of the supplier when such information may be useful to customers or business partners. CSCs are usually presented, in tabular format toward the end of the description, along with the trust service criteria to which each CSC relates. Entity management may request the practitioner's assistance when determining how to present the CSCs in the description. The practitioner can provide examples of CSC disclosures made by other entities and make recommendations to improve the presentation of the CSCs in the description. *Inclusive method.* In some situations, entity management may wish to present the relevant processes and controls of the supplier in its description either to meet the common information needs of users or because of the significance of the supplier's role in the process. This method of presentation is known as the *inclusive method*. Under the inclusive method, the relevant aspects of the supplier's infrastructure, software, people, procedures, and data are considered part of the entity's system; therefore, they are disclosed in the description and subject to the practitioner's examination procedures. The description separately identifies controls at the entity and controls at the supplier. However, there is no prescribed format for differentiating between the two. When the inclusive method is used, supplier management is also a responsible party in the examination. Because of the additional complexities involved with the use of the inclusive method, entity and supplier management usually agree on the use of the inclusive approach during engagement acceptance. *Other matters.* An entity that uses multiple suppliers may prepare its description using the carve-out method for one or more suppliers and the inclusive method for others. Regardless of the method entity management selects, the description needs to disclose controls designed to provide reasonable assurance that the entity's system objectives are achieved, which include

	controls that the entity uses to monitor the services provided by the supplier. Such monitoring controls may include a combination of the following: • Quality control testing of inputs received • Testing of controls at the supplier by members of the entity's internal audit function • Reviewing and reconciling output reports • Holding periodic discussions with supplier personnel and evaluating supplier performance against established service level objectives and agreements • Making site visits to the supplier • Inspecting attestation reports on the supplier's system • Monitoring external communications, such as complaints from customers, relevant to the products or services provided by the supplier
DC 9: Any specific applicable trust services criterion that is not relevant to the system and the reasons it is not relevant	If one or more applicable trust services criteria are not relevant to the system being described, entity management includes in the description an explanation of why such criteria are not relevant. For example, an applicable trust services criterion may not be relevant if it does not apply to the production, manufacturing, or distribution services provided by the entity. Assume customers — not the entity — collect personal information from the customers' consumers. For example, a seller of an implantable medical device uses an entity to implement the specific software configuration of electronic medical devices for each patient. The medical information for each patient is provided by the patient's physician to the seller, who then forwards the information to the entity for the configuration data to be created and implemented on the device. When the description addresses

	controls over privacy, entity management would not disclose in its description the customers' controls over collection; however, the reason for that omission would be disclosed. In contrast, the existence of a policy prohibiting certain activities is not sufficient to render a criterion not applicable. For example, when the description addresses controls over privacy, it would be inappropriate for entity management to omit from the description disclosures of personal information to third parties based only on the fact that the entity's policies forbid such disclosures. Instead, the description would describe the policies and related controls for preventing or detecting such disclosures.
DC 10: Significant changes during the period addressed by the description[13] to the entity's system and controls that are relevant to the achievement of the entity's system objectives	Significant changes to be disclosed are those that are likely to be relevant to a broad range of users. Disclosure of such changes is expected to include an appropriate level of detail, such as the date the changes occurred and how the system differed before and after the changes. Examples of significant changes to a system include the following: • Changes to the production processes, including those that result from changes to product specifications • Changes to IT and security personnel • Changes to IT processes, IT architecture and applications, and the processes and system used by suppliers • Changes to legal and regulatory requirements that could affect system requirements • Changes to organizational structure resulting in a change to internal control over the system (for example, a change to the legal entity) • Changes to the risk assessment and controls monitoring processes resulting from the failure of controls designed to

[13] When the description addresses only the suitability of design of implemented controls as of a point in time, this criterion is not applicable.

	achieve product specifications, commitments, and requirements Disclosures about significant changes to the system are only made to the extent that they relate to the trust services category or categories addressed by the description.

Effective Date

.31 The description criteria in this document are effective when issued.

Appendix — Glossary

For purposes of this document, the following terms have the meanings attributed as follows:

applicable trust services criteria. The criteria codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, which is used to evaluate controls relevant to the trust services category or categories included within the scope of the examination.

board or board of directors. Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of an entity's infrastructure, software, people, procedures, and data used to produce, manufacture, or distribute the product. When systems for multiple services share infrastructure, software, people, procedures, and data, the systems will overlap; however, the boundaries of each system will differ.

business partner. An individual or business (and its employees), other than a supplier, who has some degree of involvement with the entity's business dealings or agrees to cooperate, to any degree, with the entity (for example, a computer manufacturer who works with another company who supplies it with parts).

carve-out method. The method of addressing a supplier's controls, when such controls affect the entity's ability to achieve its system objectives, in which the components of the supplier's system used to provide products or services to the entity are excluded from the description of the entity's system and the scope of the examination. In this case, however, the description identifies (1) the nature of the products or services provided by the supplier; (2) the types of controls expected to be performed at the supplier that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives were achieved; and (3) the controls at the entity used to monitor the effectiveness of the supplier's controls.

complementary supplier controls. Controls that entity management assumed, in the design of the entity's system, would be implemented by the supplier and that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives would be achieved.

complementary customer controls. Controls that entity management assumed, in the design of the entity's system, would be implemented by customers and that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives would be achieved.

criteria. The benchmarks used to measure or evaluate the subject matter.

inclusive method. The method of addressing a supplier's controls, when such controls affect the entity's ability to achieve its system objectives, in which the components of the supplier's system includes a description of (*a*) the nature of the products or services provided by the supplier and (*b*) the components of the supplier's system for providing products or services to the entity, including the supplier's controls that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's system objectives were achieved. (When using the inclusive method, controls at the supplier are subject to the practitioner's examination procedures because the supplier's system components are included in the description.)

information life cycle. The collection, use, retention, disclosure, disposal, or anonymization of confidential or personal information within well-defined processes and informal ad hoc procedures.

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance that the entity's objectives relating to operations, reporting, and compliance are achieved.

personal information. Information that is about, or can be related to, an identifiable individual.

privacy notice. A written communication by entities that collect personal information to the individuals about whom personal information is collected that explains the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals

have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When an entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

practitioner. As used in this document, a CPA who performs a SOC for Supply Chain examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

service commitments. Declarations made by entity management to customers and others (such as business partners) about the product, production, manufacturing, or distribution specifications. Entities may also make commitments about other matters, such as (a) whether system controls conform to other standards and criteria or (b) a product's performance against specifications and product availability.

SOC for Supply Chain examination. An examination engagement to report on whether (*a*) the description of the entity's system is presented in accordance with the description criteria, and (*b*) the controls were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria based on guidance contained in the AICPA Guide *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System.*

subsequent events. Events or transactions that occur after the specified period addressed by the description but prior to the date of the practitioner's report, which could have a significant effect on the evaluation of whether the description is presented in accordance with the description criteria or whether controls were effective to provide reasonable assurance that the entity's system objectives were achieved based on the applicable trust services criteria.

system. Refers to the infrastructure, software, procedures, and data that are designed, implemented, and operated by people relevant to the production, manufacturing, or distribution of products.

system components. Refers to the individual elements of a system, which may be classified into the following five categories: infrastructure, software, people, procedures, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and could result in an entity's failure to achieve its system objectives. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems, (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data, or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of entity management to prevent or reduce the impact of a system event on the entity's achievement of its system objectives.

system requirements. Specifications about how the system should function to (*a*) meet the entity's commitments to customers and others (such as customers' customers); (*b*) meet the entity's commitments to suppliers and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

supplier. An individual or business (and its employees) that provides goods (such as raw materials, components, subassemblies, or other goods) or services to the entity.